7 Implications of the USA Patriot and Sarbanes–Oxley Acts for Hospitals

Operational Policies for Affected Health Care Organizations

David Edward Marcinko and Hope R. Hetico

CONTENTS

INTRODUCTION

In the wake of the September 11, 2001, terrorist attacks against the United States, the U.S. Congress passed Public Law 107-56, whose short title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001."

Also, because of well-publicized scandals involving Enron Corporation and its auditor, Arthur Andersen, the U.S. Congress passed Public Law 107-204, whose short title is "The Sarbanes–Oxley Act of 2002." Both the USA PATRIOT Act and the Sarbanes–Oxley Act contain sections that affect some hospitals and health care organizations.

The purpose of this chapter is to determine the financial and strategic management implications of the USA PATRIOT Act and the Sarbanes–Oxley Act for affected hospitals and health care organizations.

In order to accomplish this, we will focus on the legislation itself, the financial literature concerning the legislation, and the business literature concerning the impact of these two laws on the strategic management of hospitals.

THE USA PATRIOT ACT

The USA PATRIOT Act comprises sections covering a variety of topics. Much of the act revises or updates laws already in the United States Code (U.S.C.) in order to better coordinate efforts against terrorism. It is complemented by Executive Order #13224 and U.N. Security Council Resolution #1373, as monitored by the Office of Foreign Assets Control (OFAC) through its Specially Designated Nationals (SDN) list and Terror Exclusion List (TEL).

However, several other pieces of legislation applicable to hospitals and health care organizations have arisen because of the electronic age. For example, the Internet Spyware Prevention Act of 2005, H.R. 744 (I-SPY Act), passed by the U.S. House of Representatives on May 23, 2005, criminalizes unauthorized spyware, phishing, or other methods of obtaining sensitive personal health or other information without consent; it forbids the bringing of a civil action under the law of any state if such action was premised in whole or in part on the use of illegally obtained protected information.

As is the case with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the USA PATRIOT Act, protected information defined in the I-SPY Act includes first and last names, home or other physical addresses, e-mail addresses, telephone numbers, Social Security numbers, tax identification numbers, driver's license numbers, passport numbers, other government-issued identification numbers, credit card numbers, bank account numbers, and passwords or access codes associated with credit card, insurance company, hospital, or bank accounts. The I-SPY Act does not apply to government agencies involved in national security operations and investigations.

President George W. Bush also signed the USA PATRIOT Improvement and Reauthorization Act into law on March 9, 2006. This legislation continued the authorization for intelligence and law enforcement officials to share information and use the same tools against terrorists that had been granted in the original Act. According to the President:

> The law . . . will improve our nation's security while we safeguard the civil liberties of our people. The legislation strengthens the Justice Department so it can better detect and disrupt terrorist threats. And the bill gives law enforcement new tools to combat threats to our citizens from international terrorists. . . .

In early 2007, Senator Mark Pryor introduced the Counter Spy Act to make it illegal to implant spyware on a personal computer (PC) without consent. Spyware allows one to duplicate Web sites, including financial, health care, or retail sites, where personal medical records or financial information such as credit card numbers and insurance information is stored. It is usually downloaded without user knowledge during another software download or by simply clicking on a link ("drive-by downloading"). Once downloaded, it is almost impossible to remove.

In fact, an AOL study revealed that 80% of all computers in its test group were infected and that 89% of the users of those computers were unaware of it. The Counter Spy Act of 2007 also provides that the Federal Trade Commission (FTC) enforce the law as if a violation was an unfair

or deceptive practice. The agency would have authority to bring civil and criminal penalties (fines and/or imprisonment for up to 5 years) for violations.

In addition, late in 2007, the Committee on Energy and Commerce passed two additional bills designed to protect Americans from invasive Internet spyware and Social Security number theft. The first was H.R. 964, the Securely Protect Yourself Against Cyber Trespass Act (the Spy Act); the second was H.R. 948, the Social Security Number Protection Act of 2007.

The Spy Act shields Internet users, doctors, and patients from under-the-radar spyware programs that secretly invade PCs and monitor online activity. The Act requires software distributors and advertisers to notify and require consent from consumers and patients before programs can be downloaded from the Internet. Offenders could be assessed a fine of up to $3 million for each unfair or deceptive spyware act and up to $1 million for each violation relating to the collection of personal information without notice and consent.

The Social Security Number Protection Act is intended to protect patients and consumers from the ever-increasing problem of identity theft. The legislation restricts the sale, purchase, and use of Social Security numbers except in situations approved by the FTC, such as for law enforcement or health purposes. Violators would be fined $11,000 per infraction, up to $5 million.

At first blush, the USA PATRIOT Act and these legislative derivatives seem to have very little to do with hospitals, health care organizations, or the medical industrial complex; however, upon closer inspection, several sections appear to be relevant to the hospital and health care industry.

Prevention and Detection of Money Laundering

Title III of the USA PATRIOT Act is entitled the "International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001." The purposes of the act are "to prevent, detect, and prosecute money laundering and the financing of terrorism."

Once again, a casual reading does not suggest that this is relevant to the hospital industry. However, the definition of a financial institution is quite broad and may include some health insurance companies. The mergers, acquisitions, and restructuring that occur frequently in the health care industry have the potential to suddenly create anti-money laundering responsibilities for accountants since the responsibilities may apply across the entire organization.

"Responsibilities in a money laundering program may include

- Internal policies, procedures, and controls
- The designation of a compliance officer
- Ongoing employee training programs
- An independent audit program to test the programs"

Should there be a reference citation for this direct quote?

Thus, hospital, physician, and nurse-executives should ascertain whether their organization has anti-money laundering responsibilities, and if so, identify a designated compliance officer and determine the exact nature of any responsibilities under the anti-money laundering program.

Preparedness for Biological and Chemical Attacks

Title X of the USA PATRIOT Act contains several calls for strengthening the public health system. Section 1013(a)(4) calls for "enhanced resources for public health officials to respond to potential bioterrorism attacks." Section 1013(a)(6) calls for "greater resources to increase the capacity of hospitals and local health care workers to respond to public health threats."

Prior to September 11, 2001, the capacity of hospitals to respond to biological and chemical attacks by terrorists was quite limited. A survey of 186 hospitals concluded that hospital emergency departments (EDs) are generally not prepared to respond to biological or chemical attacks. Further, a hospital must have a plan in order to develop the capacity to respond to biological and chemical attacks.

Strictly speaking, however, hospital, ED, and health care organizational preparedness plans are not as directly encumbered by the USA PATRIOT Act, the Department of Homeland Security's Chemicals of Concern (COC) List, or the various steps of its Section 550 Program as some other industries. The COC guidelines are particularly pertinent for the agricultural industry, which is a heavy user of noxious and explosive chemicals like chlorine, nitrates, sulfur, and organophosphates. If you are not sure whether a substance is potentially toxic or covered under Title X of the USA PATRIOT Act, contact EPA's Risk Management Profile hotline at 1-800-424-9346 or 703-412-9810. For further details, see www.EPA.gov.

Nevertheless, hospitals and health care organizations may have other sources of contaminants, such as those listed below.

Mercury. Mercury is a heavy metal used in several products in hospitals, like thermometers, computers, batteries, and fluorescent lamps. The metal can be toxic to the nervous system and cause problems with memory, information processing, attention, language, and fine motor skills.

Dioxin. Dioxins are toxic chemical compounds formed during the burning of hospital waste. The chemicals are also found in products with polyvinyl chloride (PVC), a plastic polymer. Dioxin has been linked to the development of several kinds of cancer. In humans, dioxin exposure may cause changes in the immune system and in the levels of some hormones.

DEHP. Di (2-ethylhexyl) phthalate (DEHP) is a plasticizer added to PVC products to soften and increase flexibility of some medical devices [like intravenous (IV) bags and tubing]. It does not bind well with the PVC and can leach out of the product and into the body. DEHP may be toxic to the liver, lungs, and developing male reproductive system.

Volatile organic compounds (VOCs). VOCs are chemicals emitted as gases from liquid or solid products. Some of the most common types of VOCs are in formaldehyde, pesticides, solvents, and cleaning agents. Exposure may cause irritation of the eyes, nose, or throat; breathing problems; headache; and nausea. VOCs may be toxic to the liver, kidneys, and central nervous system.

Glutaraldehyde. Glutaraldehyde is a colorless, oily liquid used to cold-sterilize medical instruments and some types of hospital equipment. It is also used in labs and in the processing of X-ray films. Exposure can irritate the airways and cause breathing problems, nosebleed, burning of the eyes, headache, or nausea. Contact with the skin can lead to a rash or hives.

For some time now, the Joint Commission (formerly the Joint Commission on Accreditation of Healthcare Organizations, known as JCAHO) has also required hospitals to have a disaster preparedness plan mimicking the USA PATRIOT Act. For example, before September 11, 2001, only one in five hospitals had a response plan specifically tailored for biochemical attacks. By February 2005, two out of three hospitals had response plans for biochemical attacks. Today, such disaster plans are almost uniformly present to one degree or another, although successful implementation may be suspect.

After the terrorist attacks of September 11, 2001, "disaster preparedness" evolved into something that could more accurately be described as "emergency preparedness." Experience in New York and Virginia has shown that there will be spillover outside the immediate geographic areas affected by a terrorist attack, which will affect suburban and rural hospitals. Thus, the emphasis in emergency preparedness is on the coordination and integration of organizations throughout the local system. Hospitals therefore need to revise existing plans for disaster preparedness to reflect the realities of potential terrorist threats.

Mitigation against risk is essential to safeguard the financial position of a hospital. Hospitals can mitigate risks by developing an emergency preparedness plan. The hospital should start by identifying

possible disaster situations such as earthquakes and biological or chemical attacks that could affect the facility. Next, the hospital should identify the potential damages that could occur to structures, utilities, computer technology, and supplies. After that, the hospital should use resources currently available to safeguard assets and then budget to acquire any additional materials or alterations required to secure the facility. Using this approach, Olive View Medical Center in Los Angeles lowered recovery costs from $48 million after an earthquake in 1971 to $6.6 million after another earthquake in 1994.

Should there be a specific reference to where this passage is in the Act, as on page 6? Is this from Title X?

"Hospitals can take several steps to mitigate even in the absence of significant funding:

- First, hospitals can establish links with 'first responders' such as local law enforcement, fire departments, state and local government, other hospitals, emergency medical services, and local public health departments.
- Second, hospitals can establish training programs to educate hospital staff on how to deal with chemical and biological threats.
- Third, hospitals can make changes in their information technology to facilitate disease surveillance that might give warning that an attack has occurred. Information technology may be useful in identifying the occurrence syndromes such as headache or fevers that might not be noticed individually but in the aggregate would signal that a biological or chemical agent had been released.
- Fourth, hospitals may be able to acquire access to staff and equipment to respond to biological and chemical attack through resource-sharing arrangements in lieu of outright purchases."

In addition to preparedness for an attack within its catchment area, a hospital must be prepared for an attack on its own facility. Hospitals should assess the vulnerability of the heating, ventilation, and air conditioning (HVAC) systems to biological or chemical attack. The positioning of the air intake vents is especially important because intakes on roofs are fairly secure as compared to intakes on ground level.

One way to increase security is to restrict access to the facility. Some hospitals are using biometric screening to restrict access to their facilities. Biometric screening identifies people based on measurements of some body part such as a fingerprint, handprint, or retina. The advantage of this approach is that there are no problems with forgotten badges, and biometric features cannot be shared or lost like cards with personal identification numbers (PINs).

In preparing for a possible attack, hospitals should also examine the federal, state, and local laws that might affect their response to a biological or chemical attack. Unfortunately, there is no central source of legislation, and an extensive search of many sources might be required to determine the legal constraints.

Obviously, upgrading emergency preparedness plans costs money. Trustees and financial officers should always be alert to federal, state, or local funds that may come available to defray some of the costs of preparedness. Some good places to search for information would be the Department of Health and Human Services (DHHS; see www.os.dhhs.gov) and the Centers for Disease Control and Prevention (see www.cdc.gov and www.govbenefits.gov/govbenefits_en.portal). Other private sources are www.patriotactresearch.com and patriotact.com.

Protection of Critical Infrastructures

Title X of the USA PATRIOT Act also contains Section 1016, entitled "The Critical Infrastructures Protection Act of 2001." It acknowledges that the defense of the United States is based on the functioning of many networks and that these networks must be defended against attacks of both a physical and a virtual nature. Section 1016 specifies that actions necessary to carry out policies designed to protect the infrastructure will be based on public and private partnerships between the government and corporate and nongovernmental agencies. Further, it specifies that these actions are designed to ensure the continuity of essential government functions under all circumstances. Toward

this end, the act establishes a National Infrastructure Simulation and Analysis Center (NISAC) to support counterterrorism, threat assessment, and risk mitigation. NISAC will acquire data from governments and the private sector to model, simulate, and analyze critical infrastructures including cyber, telecommunications, and physical infrastructures.

Attacks on the Internet and attacks on the information systems of hospitals have already occurred in significant numbers and are likely to continue. As a result of the USA PATRIOT Act, agencies to combat information technology (IT) terrorism have been created, such as the Critical Infrastructure Protection Board and the Critical Infrastructure Assurance Office. An Information Sharing and Analysis Center (ISAC) has been created to gather, analyze, and distribute information on cyber threats and vulnerabilities, provide alerts, and develop response plans. An ISAC for health care that will compile industry best practices, develop security systems, and establish a governance structure to which health systems can turn is under development.

The increasingly complex relationships among layers of hardware and software mean that new avenues for exploitation appear on almost a daily basis. Also, increased connectivity among computers means that the effects of attacks can be far reaching. One interesting consequence of the USA PATRIOT Act is that some cyber attacks can now be defined as acts of terrorism. As a practical matter, legal recourse against most attacks is of no use since laws tend to apply only locally and cyber attacks can come from anywhere in the world. As a result, most organizations concentrate on technical defenses to protect their infrastructure. However, efforts to protect computer systems may not be entirely defensive. One mode of defense is to monitor for intrusions, trace the source of intrusions, and aggressively attack and shut down the server of an intruder.

Financial Implications of USA PATRIOT Act for Hospitals

The financial implications of the USA PATRIOT Act are summarized in Table 7.1.

Health Insurance Implications of the USA PATRIOT Act on Hospitals

With the recent popularity and growth of health savings accounts (HSAs) and/or medical savings accounts (MSAs), compliance with the USA PATRIOT Act has become an important issue for these new, hybrid health insurance products that place financial services organizations into relationships with shared information institutions such as hospitals, health care organizations, medical clinics, and patient clients.

TABLE 7.1
Financial Implications of USA PATRIOT Act

Activities That May Require Increased Funding	Potential Return on Investments
Prevention of money laundering: —Training for staff —Detection software	Prevention or mitigation of financial losses and criminal liability
Preparedness for biological and chemical attack: —Training for staff —Software for monitoring, analysis, and reporting	Prevention or mitigation of losses due to lapses in emergency preparedness
Preparedness for cyber attack: —Training for staff —Protective and counterattack software	Prevention or mitigation of losses due to lapses in computer security affecting medical or financial information
Increased physical security for facility	Prevention or mitigation of losses due to lapses in physical security

This happens because many, perhaps even the majority of, HSAs, MSAs, and high-deductible health care plans are opened online, as patients and insurance company clients use Internet search engines to find the "best" policy type to meet their needs. Appropriately, banks, health care entities, and hospitals are working with insurance companies, trust companies, and broker-dealers to offer identity-compliant and integrated HSAs and MSAs. Verifications that these clients are who they claim to be are as paramount as monitoring their activity.

Health care organizations may meet these requirements of the USA PATRIOT Act by adhering to its Customer Identification Program (CIP) and anti-money laundering requirements. Section 314(b) of the Act permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. This USA PATRIOT Act derivative partially accomplishes this through three critical goals:

- First, it gives investigators familiar tools to use against a new threat.
- Second, it breaks down a wall that has prevented information sharing between agencies.
- Third, it updates U.S. laws to respond to the current Internet environment.

On October 1, 2003, Section 326 (CIP) of the Act went fully into effect, requiring the implementation of reasonable procedures to verify the identity of new customers and certain existing customers opening a new account.

Section 3261 of the USA PATRIOT Act also requires banks, savings associations, hospital and medical union credit unions, and certain non-federally regulated banks to have the CIP fully implemented. Broker-dealers in securities are subject to similar but slightly different rules.

For additional compliance, the USA PATRIOT Act also amended the Bank Secrecy Act to give the federal government enhanced authority to identify, deter, and punish money laundering and terrorist financing activities.

The passage of the USA PATRIOT Act, and these important derivatives, means that hospitals must be more vigilant about laws concerning money laundering, reporting of disease and quarantine, and cyber attacks. This means that more funds may be needed in order to combat money laundering, biological and chemical attacks, and security of all kinds, particularly IT security. Furthermore, many of the changes necessary to improve preparedness can be made with fairly small outlays of funds, and more funding provided by the federal government may eventually materialize. Whatever outlays are required now may result in very large savings later if hospital assets are safeguarded against attacks of virtual or real assets.

USA PATRIOT Act's Impact Since Inception

Almost a decade after passage of the USA PATRIOT Act, little is known about how it is being used to track terrorists, health care organization activity, or innocent Americans.

For example, the Department of Justice (DOJ) foiled numerous attempts to learn how the Administration has deployed the new tools granted under the Act. Even Congressional hearings several years ago, during the tenure of Attorney General John D. Ashcroft, yielded virtually no new information about the number of times individuals' library records were sought or how many court orders were obtained to monitor someone's computer activities or conduct surveillances on U.S. citizens. DOJ officials claimed that even generic numbers are classified and are provided confidentially only to congressional intelligence committees.

Unfortunately, the terrorist incidents of July 2007 in the United Kingdom implicated eight medical workers (doctors, medical students, lab technicians) from a clandestine Al-Qaeda sleeper cell. Although the violence was successfully thwarted, the fact that all were tied to the British National Health Service (NHS) indicates the international nature of such threats and the need to carefully screen the foreign-trained physicians on whom we increasingly rely.

Edit OK for NHS acronym? No National Healthcare System found.

In 2009, Attorney General Eric Holder reauthorized the PATRIOT Act and reiterated his support for warrantless wiretapping:

> "There are certain things that a president has the constitutional right that the legislative branch cannot impinge upon."

PATRIOT ACT EXTENSION

In May 2011, President Barack Obama signed into law a 4-year extension for parts of the PA's controversial domestic surveillance law, just before the provisions were to expire. The three provisions that were extended allowed authorities to use roving wiretaps, conduct court-ordered searches of business records, and conduct surveillance of foreign nationals who may be acting alone in plotting attacks.

Frequently Asked USA PATRIOT Act Questions

Q: What is Executive Order 13224?
A: Signed by President George W. Bush in September 2001, the order authorizes the Executive Branch to block the property of, and prohibit transactions with, persons who commit, threaten to commit, or support terrorism.
Q: What is U.N. Security Council Resolution 1373?
A: U.N. Security Council Resolution 1373, adopted at the end of September 2001, declares that all states (or nations) shall prohibit their nationals or any persons and entities within their territories from making any funds available for terrorism. In the broad wording of Resolution 1373, financial assets, economic resources, or financial or other related services shall not be made available, directly or indirectly, for the benefit of persons who commit, attempt to commit, facilitate, or participate in the commission of terrorist acts.
Q: To whom do the USA PATRIOT Act laws apply?
A: All U.S. citizens, permanent resident aliens, and entities and organizations located in or out of the United States (including any subsidiary or foreign offices overseas) must comply with the USA PATRIOT Act, Executive Order 13224, and Office of Foreign Assets Control regulations. Further, U.N. Security Council Resolution 1373 and other resolutions have the force of international law binding on all member states.
Q: What is the Office of Foreign Assets Control (OFAC)?
A: OFAC is a division of the U.S. Department of the Treasury. It helps enforce sanctions against terrorist organizations, drug traffickers, money launderers, and noncooperative foreign countries.
Q: What is the OFAC-SDN list?
A: The OFAC Specially Designated Nationals (SDN) and blocked persons lists are U.S. government lists of individuals and organizations identified as terrorists or otherwise associated with terrorism, drug trafficking, and money laundering.
Q: What is the Terror Exclusion List (TEL)?
A: TEL is the U.S. Department of State's list of organizations identified as terrorists or otherwise associated with terrorism for immigration purposes.
Q: What sanctions do hospitals face if material support is given to watch-listed parties?
A: The health care organization faces the possibility of having its assets frozen and its tax-exempt status revoked, if it exists. There is also the potential for criminal and civil penalties. In addition, administrators, managers, and executives may face penalties.
Q: Do current USA PATRIOT Act laws define "material support"?
A: The Antiterrorism and Effective Death Penalty Act broadly defines *material support* as "currency or monetary instruments of financial securities, financial services, lodging, training, expert advice or assistance, safe houses, false documentation or identification, communications,

equipment, facilities, weapons, lethal substances, explosives, personnel transportation, and other physical assets, except medicine or religious materials."

Q: Should a health care entity amend funding support agreements to comply with the USA PATRIOT Act?

A: Yes, it is recommended that any grant or funding agreement include prohibitions against violence or terrorist activities.

THE SARBANES–OXLEY ACT

In response to the failure of public accounting firms to detect corporate fraud, the Sarbanes–Oxley Act requires rotation of auditors to maintain independence, increases accountability for corporate fraud, and prescribes changes in governance, internal controls, ethics, and disclosure.

Previously, the Treadway Commission Report (*Fraudulent Financial Reporting: 1987–1997—An Analysis of U.S. Public Companies*) was its equivalent, sponsored by The Committee of Sponsoring Organizations (COSO) to provide:

> …an analysis of financial statement fraud occurrences. While the work of the National Commission on Fraudulent Financial Reporting in the mid-1980s identified numerous causal factors believed to contribute to financial statement fraud, little empirical evidence existed about other factors related to instances of fraud prior to release of the 1987 report (NCFFR, 1987). Thus, COSO commissioned this research project to provide information that can be used to guide future efforts to combat the problem of financial statement fraud and to provide a better understanding of financial statement fraud cases.

In other words, the Treadway Commission Report first spelled out the whys and wherefores of internal control as the original de facto standard for defining such corporate controls.

Unfortunately, many leaders, including some hospital administrators and physician-executives, still think that the Sarbanes–Oxley Act applies only to investor-owned or publicly traded health care organizations. While this is partially true, the legislation does contain some provisions that are applicable to nonprofit hospitals. Also, moral persuasion is increasing in the health care sector.

For example, provisions relating to the retaliation against hospital whistleblowers and to medical document retention and/or destruction are applicable to nonprofit health care entities as well as their for-profit counterparts. Moreover, nonprofit hospitals that issue tax-exempt bonds and/or rely on bond ratings from services such as Moody's and Fitch have to comply with Sarbanes–Oxley provisions to obtain and maintain those bond ratings.

In addition, Sarbanes–Oxley provisions do have some implications for all hospitals, regardless of ownership type.

Governance

Title III, Section 302, is entitled "Corporate Responsibility for Financial Reports." This section requires that the principal officers and financial officers sign the financial report, certify that the report contains no false statements, and certify that the report is materially correct. They face stiff penalties if any of these certifications are found to be untrue.

The implications extend beyond just Centers for Medicare & Medicaid Services fraud, civil penalties, and imprisonment. Hospitals are now largely operated by public entities and thus file financial forecasts and financial statements. Periodic statutory financial reports are to include certifications that

- The signing officers have reviewed the report.
- The report does not contain material untrue statements or omissions considered misleading.

- The financial statements and related information fairly present the financial condition and the results in all material respects.
- The signing officers are responsible for internal controls, have evaluated these internal controls within the previous 90 days, and have reported on their findings.
- A list of all deficiencies in the internal controls is provided, as is information on any fraud that involves employees who are involved with internal activities.
- Any significant changes in internal controls or related factors that could have a negative impact on the internal controls are documented.

The Sarbanes–Oxley Act also establishes an independent governing commission, which is required to study and report on the extent of off-balance transactions. The commission is required to determine whether generally accepted accounting principles or other regulations result in open and meaningful reporting.

The Sarbanes–Oxley Act puts a new premium on the independence of board members and the importance of the audit, compensation, and nominating committees. As a result, boards will be more likely to compensate directors fairly in light of their increased responsibilities. Further, boards will likely pay more attention to the education of board members.

Boards and officers should seek to do more than just comply with the Sarbanes–Oxley Act. Compliance can lay the groundwork for "enterprise risk management," which identifies potential obstacles to accomplishing strategic objectives and thereby improves performance.

As a result of the Sarbanes–Oxley Act, even not-for-profit hospitals would do well to upgrade the membership of the board in terms of financial expertise and independence, update bylaws, and establish audit committees. Further, hospital boards should be making more sophisticated financial analyses examining revenue position, cost position, market strength, and the adequacy of capital. Last, hospital boards should be smaller and composed of people with more financial skill who are adequately compensated for their service.

Internal Controls

The Sarbanes–Oxley Act, Title III, Section 302(a)(4)(A)–(D), indicates that the officers signing the financial reports are responsible for

- Establishing and maintaining internal controls
- Designing the internal controls so that material information relating to the issuer is made known to the officers
- Evaluating the effectiveness of internal controls within 90 days
- Presenting in the report their conclusions about the effectiveness of internal controls

Title IV, section 404, requires each annual report to contain an internal control report that states that it is the responsibility of management to establish and maintain an internal control structure and to provide an assessment of the effectiveness of that structure.

With regard to corporations in general, the compliance burden of these requirements for internal controls is quite substantial and will fundamentally change the way corporations do business internally and the way they do business with their auditors. Revenue recognition is a particularly important issue in the new internal controls, and corporations should consider forming a revenue recognition committee to serve as a primary tool of internal control. Organizations should consider purchasing internal control software that is robust and flexible so that compliance is sustainable even when business operations change significantly.

With regard to hospitals, the Sarbanes–Oxley Act will cause nearly all hospitals, regardless of ownership type, to institute internal controls to ensure the accuracy of financial reports, even though it is not currently mandatory for not-for-profit hospitals. However, most executives expect

the requirements to become mandatory for not-for-profit hospitals, and many hospitals have already begun implementing internal controls to assure the accuracy of financial reports. Further, compliance programs in hospitals should be considered not optional but required. There will likely be an expansion of the functions of the compliance officer, and hospitals will be more likely to establish procedures for receiving complaints and tips from anonymous whistleblowers. New software for hospitals can provide continuous auditing to monitor for Sarbanes–Oxley Act violations.

Ethics

Title IV of the Sarbanes–Oxley Act is entitled "Enhanced Financial Disclosures," and Section 406 is entitled "Code of Ethics for Senior Financial Officers." Section 406 calls for ethical handling of actual or apparent conflicts of interest, full disclosure in the financial reports, and compliance with government rules and regulations.

With regard to corporations in general, the ethics prescribed in the Sarbanes–Oxley Act cover the handling of conflicts of interest, accurate disclosure in reports, and compliance with laws and rules. The Sarbanes–Oxley Act requires publicly traded companies to disclose whether they have adopted a code of ethics for senior financial officers. The Sarbanes–Oxley Act may have the result of forcing financial officers to pay more attention to the accuracy of financial reporting and the evaluation of business risk. Further, it will force corporations to develop cultures that reinforce corporate values, to carefully assign responsibilities, and to reward employees who perform ethically and effectively.

With regard to hospitals, although most hospitals already have a Joint Commission code of ethics that addresses a different set of ethical issues for their board, they would also do well to upgrade their codes to reflect the Sarbanes–Oxley Act. There is some evidence that voluntary compliance with regard to the code of ethics has already taken place to ensure their access to funds by strengthening their reputation.

Disclosure

Title IV, Section 409, is entitled "Real Time Issuer Disclosures." It requires disclosure to the public "on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations . . . (that) is necessary or useful for the protection of investors and in the public interest."

With regard to corporations in general, most rely too much on the annual budget as the only performance management tool. The problem is that few organizations are able to identify the cost of servicing a key customer and the revenue associated with that customer. Thus, most organizations and most financial officers would not easily be able to identify the impact of losing a key customer, and thus, they would not be likely to recognize and disclose a key loss. Organizations need to maintain records that show a high-level activity layer that shows the relationship between the revenues and costs for key customers.

Furthermore, financial statements published and disclosed by regulated health care entities are required to be accurate and presented in a manner that does not contain incorrect statements. These financial statements must include all material off-balance-sheet liabilities, obligations, or transactions. Regulated hospitals and health care organizations are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement must assess the effectiveness of such internal controls and procedures.

A financial expert and/or registered accounting firm must in the same report attest to, disclose, and report on the assessment of the effectiveness of the internal control structure and procedures for financial reporting.

Regulated health care entities are required to disclose to the public, on an urgent basis, information on material changes in their financial condition or operations. These disclosures are to be presented in terms that are easy to understand, supported by graphic presentations of trend and qualitative information as appropriate.

With more specific regard to hospitals, the Sarbanes–Oxley Act could lead to voluntarily expanded disclosure in not-for-profit hospitals. Some hospitals have already voluntarily taken a stricter stance on disclosure.

Hospitals may be required to take stricter stances on disclosure by the attorney general of their respective states, if not directly by the Sarbanes–Oxley Act. Hospitals should do the following:

- "Adopt a strict conflict of interest disclosure statement and policy . . .
- Develop an unambiguous definition of what constitutes conflict of interest . . .
- Develop and use solid criteria for selecting new board members . . .
- Treat prospective physician board members like all board members."

Financial Implications of the Sarbanes–Oxley Act for Hospitals

Although the Sarbanes–Oxley Act was passed in response primarily to events that took place outside the health care industry, its passage has nevertheless affected the financial management of some hospitals. The effect of the Sarbanes–Oxley Act on the health care industry can be explained by the concept of "isomorphism." DiMaggio and Powell identify the concept of "mimetic isomorphism," whereby organizations adopt the form of other organizations in society to obtain legitimacy in the eyes of society.

Thus, although the letter of the law currently affects only publicly traded corporations, it creates social pressures that affect not-for-profit organizations such as hospitals.

This social pressure may soon metamorphose into legal pressure or "coercive isomorphism." States and their attorneys general may soon pass additional or more stringent legislation requiring not-for-profit hospitals to conform more exactly to the Sarbanes–Oxley standards. Some bond markets are also pressuring not-for-profit hospitals to adhere to Sarbanes–Oxley standards. Although insurers could penalize hospitals that do not comply with the Sarbanes–Oxley Act, there are as yet no examples of this happening.

The financial implications of the Sarbanes–Oxley Act are presented in Table 7.2.

On the one hand, the Sarbanes–Oxley Act creates a compliance burden for hospital executives. Some effort must be expended to recruit, retain, compensate, and educate more financially astute

TABLE 7.2
Financial Implications of the Sarbanes–Oxley Act

Activities That May Require Increased Funding	Potential Return on Investments
Compensation of board members	Increased safeguards against loss due to fraud or mismanagement
Education of board members	Better access to capital
Acquisition of software for more sophisticated financial analysis	Lower risk and lower cost of capital
Increased internal audit personnel	Better financial decisions due to decreased conflict of interest
Internal audit software	Better financial decisions due to increased financial acumen
Increased independent audit fees	Increased safeguards

board members to comply with the requirements for governance. Further, more time must be spent on the development of codes of ethics and cultures of compliance.

Yet something about Sarbanes–Oxley Act compliance must be working because nonprofit hospitals in North Carolina intend to voluntarily implement Sarbanes–Oxley–like internal controls, beginning in 2008. First reported by www.ManagedHealthcare.com and in the *Philanthropy Journal*, these North Carolina entities explain that they have a duty to be as transparent as possible and to demonstrate that they deserve public trust in managing contributions. No pressure for improved financial statements was cited, nor were concerns about fraud in the executive suite. To that end, the organizations require each chief executive officer (CEO) and chief financial officer (CFO) to sign off on financial statements. Audit committees also include a financial expert who is separate from the finance committee and who reports directly to the board of directors rather than to management.

Interestingly, these few are not the first nonprofit health entities to tackle Sarbanes–Oxley compliance. The University of Pittsburgh Medical Center, which is a public, nonprofit health care organization, proclaimed itself to be the first large health care system to voluntarily attain compliance with the Sarbanes–Oxley Act. Its outside auditors, Ernst & Young, certified full compliance in 2007.

Some capital outlay will probably be required to develop or acquire more sophisticated financial software that can show the relationships between revenues and costs for each major line of customers so that hospitals can comply with the higher levels of disclosure required. Further, considerable capital outlays may be required to upgrade the internal auditors' software and to pay for independent audits that will likely be more expensive due to the required rotation of auditors. Last, the requirements of the Sarbanes–Oxley Act may make some hospitals more economically risk averse, which could result in poorer financial performance.

For example, according to a report by a Sarbanes–Oxley research and compliance firm, Lord & Benoit, the average first-year cost for management assessment—with additional audit fees—was about $78,474 or nearly 14% less than the Securities and Exchange Commission (SEC) originally predicted for similar businesses.

On the other hand, there may be benefits that will accrue from the stricter burden of compliance. Stricter ethics may result in boards making decisions that are better for hospitals. Better disclosure may ultimately cause less risk to investors and provide better access to capital. More astute boards may actually make better financial decisions. Stronger internal controls may well help to avoid embarrassing and costly financial failures in hospitals.

Penalties

Sarbanes–Oxley imposes penalties of fines and/or up to 20 years' imprisonment for altering, destroying, mutilating, concealing, or falsifying records, documents, or tangible objects with the intent to obstruct, impede, or influence a legal investigation.

The legislation also imposes penalties of fines and/or imprisonment up to 10 years on any accountant who knowingly and willfully violates the requirements of maintenance of all audit or review papers for a period of 5 years.

Organizations may not attempt to avoid these requirements by reincorporating their activities or transferring their activities outside of the United States.

Example Fines

As part of a settlement arising from allegations of improper Medicare billing related to the Sarbanes–Oxley Act and others, Abraham Lincoln Memorial Hospital in Lincoln, Illinois, paid fines of $1.34 million in 2006 and entered into a 3-year corporate integrity agreement arrangement. It also agreed to maintain a compliance plan and provide information regarding the plan to the DHHS.

The settlement required no admission of wrongdoing as the hospital maintained it acted on the recommendation of outside consultants. Adequacy of patient care was not an issue in the investigation.

The Lincoln hospital case is the fourth settlement in 3 years arising from an investigation of for-profit hospital claims under the Sarbanes–Oxley Act, the False Claims Act, and/or its related derivative regulations.

Sarbanes–Oxley Act Impact Since Inception

Since enactment 10 years ago, Sarbanes–Oxley today is still perceived to have a limited, but growing, impact in driving improved corporate health care governance in 2012. There is also a belief in the nonprofit hospital industry that voluntary adoption of the Sarbanes–Oxley Act will keep Congress and state legislators at bay during a time of increased scrutiny of the tax-exempt status of hospitals.

Indeed, some nonprofit health care providers are adopting parts of the Sarbanes–Oxley Act to manage risk, achieve efficiencies, and improve performance with more effective internal controls and financial reporting methods. Additionally, board members who serve on both public company and tax-exempt boards are demanding the adoption of the Sarbanes–Oxley Act by tax-exempt health care providers. Of course, establishing a sound corporate governance environment can also result in much greater confidence in an organization, internally and externally.

A study done by FTI Consulting in 2008 showed that high-net-worth investors and financial advisors felt that corporate board members are still too closely aligned with the interests of executive management teams as opposed to shareholders. The survey of more than 200 high-net-worth investors and professional financial advisors, administered by independent research firm Affluent Dynamics, revealed that clear majorities (61% of financial advisors and 64% of high-net-worth individuals) say that boards operate in the interests of management rather than those of shareholders.

Slowly, but increasingly, hospitals, tax-exempt clinics, and other health care organizations are beginning to adopt portions of the Sarbanes–Oxley Act that affect their entities, albeit in a fragmented, "Sarbanes–Oxley Lite" approach that is becoming more substance than style. The Sarbanes–Oxley Act is also now on the radar screen of the *American Journal of Medical Quality.*

Based on such findings, for-profit health care organizations and related entities have significant work to do to reassure investors, medical executives, patients, and advisors about the effectiveness and quality of corporate governance practices and whether these practices are appropriately safeguarding hospital reputations, which both groups consider to be crucial in the creation of shareholder value.

This phrase is a bit unclear. If possible, please rephrase/clarify.

All of these findings track with a survey of institutional investors conducted just following Sarbanes–Oxley passage in 2002, which showed that a plurality of respondents (40%) did not think the bill's provisions were adequate to significantly strengthen corporate hospital accountability.

However, in the words of former health care administrator and current industry and iMBA Inc. pundit Rachel Pentinmaki, RN, MHA, CMP™ (Hon) (personal communication, Atlanta, Georgia, September 2011):

> "Although Sarbanes-Oxley has mimicked the slow start of HIPPA, but *[sic]* it has the potential to become even more important, onerous and costly to all affected hospitals and healthcare organizations."

Frequently Asked Sarbanes–Oxley Act Questions

Q: Who is a "financial expert"?

A: Anyone with education and experience as a public accountant, auditor, financial officer, comptroller or principal, and/or from a position involving similar functions.

Q: What is a "whistleblower"?
A: Any employee who provides information or assists in the investigation of any provision relating to fraud against shareholders.
Q: Are there materiality guidelines for complaints?
A: There are no materiality qualifiers in the Act. All complaints regarding accounting or internal controls or auditing reporting matters are covered.
Q: Is the audit committee required to review all complaints?
A: Yes, even though not stated specifically in the legislation.
Q: What level of complaint detail does the audit committee need to review?
A: This can vary as operational incidents may be summarized, while more serious incidents must be presented in detail for appropriate resolution.
Q: How is independence defined?
A: Independence has two definitions: (1) pertaining to an audit firm and (2) pertaining to a member of an audit committee.
Q: Can an audit firm perform a service that is a subject of the audit itself?
A: No, and audit committee members of the board cannot accept compensation or be affiliated with the issuer or a subsidiary.
Q: How should employees be notified of their ability to report Sarbanes–Oxley concerns?
A: Generally, entities should (1) post bulletin boards at all locations where other legal notices such as Worker's Compensation are posted and (2) place notices and links on company intranets or private Web sites.
Q: What else happens if an entity is not in compliance?
A: Depending on the section, noncompliance penalties range from the loss of stock exchange listing and loss of directors' and officers' (D&O) insurance to multimillion-dollar fines and imprisonment.

Tenth Anniversary of Sarbanes–Oxley

According to the 2011 Sarbanes–Oxley Compliance Survey by Protiviti, nearly 90% of respondents said the recession of 2008–2009 and the current economic malaise did not affect compliance, and half said that internal control over financial reporting has improved over the last year. This confirms a general sense that big companies especially have grown comfortable with their Sarbox processes.

Unsure of definitive acronym (also SarbOx and SARBOX); also, does this need to be defined first or can it stand alone?

Indeed, the costs of compliance continue to trend down. However, cost reductions have come over the course of 9 years. What does this mean for Dodd-Frank and other recent financial reform laws? It is hard to generalize, but part of the tremendously energetic response by the financial services and other industries—such as health care—to various pieces of Dodd-Frank legislation is driven in some part by the Sarbox experience.

CONCLUSION

In summary, both the USA PATRIOT Act and the Sarbanes–Oxley Act provide little indication in their titles that they will affect the management of hospitals or health care organizations. Nevertheless, both acts were intended to safeguard the nation and its economy. Since the health care industry is such a large and integral part of the economy, it necessarily follows that legislation designed to protect our nation and its economy will invariably have an effect on hospitals. Both acts require hospitals to analyze their activities and make capital outlays, but compliance with both acts can prevent or mitigate losses and very possibly improve financial performance.

ACKNOWLEDGMENTS

The authors would like to thank Gregory O. Ginn, PhD, MBA, CPA, Med, Associate Professor, Department Health Care Administration and Policy at the University of Nevada, for technical assistance in the preparation of this chapter.

CASE MODEL 7.1 EVAN AND THE USA PATRIOT ACT

Evan was the chief financial officer of a community hospital in San Marcos, Texas. His hospital had recently been acquired by an insurance company. As he left the hospital, he reflected on the events of the day. During a meeting of the management team, the issue of the USA PATRIOT Act had come up. Evan knew that it contained many diverse sections, and he was concerned that the legislation might affect his job duties. His grandfather, who lived in Las Vegas, had told him that some of the hospitals in Las Vegas had once been used for money laundering, and he knew that there was a money laundering section of the USA PATRIOT Act. When he asked the CEO if he thought the money laundering section might apply, the CEO laughed. He said that the money laundering in Las Vegas was concerned with illegal activities of the "Mob" and that the USA PATRIOT Act was aimed at terrorists. Besides, he added that the money laundering prevention and detection activities were designed for financial institutions, not hospitals.

Evan also asked about the section on bioterrorism and whether the community hospital had an emergency preparedness plan. The CEO responded that the hospital had a disaster preparedness plan that had been instituted after the disastrous floods that had occurred some years earlier. Further, the CEO said that the terrorists would most likely attack San Antonio because of its huge military bases or Austin because of its large population of narcissistic yuppies who could be easily terrorized. In any event, attacks on San Antonio or Austin would not likely affect San Marcos, so contingency plans were not needed.

Evan said nothing, but he felt uneasy. Instead of driving home to Buda, he drove to the library of the Texas State University and sought an authoritative interpretation of the USA PATRIOT Act from a private clearinghouse publication. He also spent some time doing a database search.

KEY ISSUES

Was the CEO correct with regard to the following assertions?

1. The USA PATRIOT Act money laundering detection and prevention sections do not apply to the hospital.
2. The USA PATRIOT Act sections on bioterrorism attacks have little relevance for the community hospital in San Marcos.

CHECKLIST 1: USA PATRIOT Act	YES	NO
Money Laundering		
Do the money laundering statutes apply to my health care organization?	o	o
Does the hospital have an anti-money laundering monitoring system?	o	o
Does the hospital have a suspicious financial activity detection system?	o	o
Does the hospital have a fraud control officer?	o	o
Does the hospital have the required internal financial controls?	o	o
Does the hospital have an independent audit program?	o	o
Does the hospital monitor and screen wire fund transfer payments?	o	o
Does the hospital have a watch list of potential offenders?	o	o
Does the hospital have and use suspicious activity reports?	o	o
Does the hospital have a new and ongoing employee training program?	o	o
Does the hospital have a supervisory policy?	o	o
Does the hospital review new vendor account documentation?	o	o
Does the hospital review and screen new corporate client accounts?	o	o

Bioterrorism		
Is the emergency preparedness plan up to date?	o	o
Have all threat sources been identified?	o	o
Have potential damages been assessed?	o	o
Have appropriate safeguards been installed?	o	o
Does the budget reflect additional safeguards needed?	o	o
Has the hospital established links to first responders?	o	o
Has the hospital instituted staff training in response to bioterrorism?	o	o
Does the information technology recognize syndromes?	o	o
Has the hospital instituted resource-sharing arrangements?	o	o
Has the hospital evaluated the vulnerability of the HVAC systems?	o	o
Does the hospital have an aggregate pool of electronic storage where the data can be easily secured, backed up, and retrieved?	o	o
If so, do you know where the data is stored and/or where it is outsourced?	o	o
Has the hospital secured access to all parts of the facility?	o	o
Has the hospital reviewed pertinent federal, state, and local laws?	o	o
Have applications been made for available funding?	o	o
Critical Infrastructure		
Do I monitor information available from the health care ISAC?	o	o
Have I provided backup records and alternate systems?	o	o
Have I evaluated software to prevent cyber attacks?	o	o
Financial Implications		
Must your health care entity comply with the Bank Secrecy Act (BSA)?	o	o
Must your hospital comply with the customer identification program (CIP)?	o	o
Are you familiar with the Office of Foreign Assets Control (OFAC)?	o	o
Are you aware of the Specially Designated Nationals (SDNs) and Terror Exclusion List (TEL)?	o	o
Internet and Electronic Security		
Are you aware of HR 744, the Internet Spyware Prevention Act of 2005 (known as I-SPY)?	o	o
Are you familiar with the Counter Spy Act of 2007?	o	o
Are you aware of HR 964, the Securely Protect Yourself Against Cyber Trespass Act?	o	o
Are you familiar with HR 948, the Social Security Number Protection Act of 2007?	o	o

CASE MODEL 7.2 CLARE AND THE SARBANES-OXLEY ACT

Clare had just graduated from the University of Texas at Austin. While taking classes in the McCombs College of Business, she had learned of the Sarbanes-Oxley Act. McCombs College instructors had paid special attention to the Sarbanes-Oxley Act since it was the financial collapse of Enron Corporation and the failure of its auditor, the Houston office of Arthur Anderson, that had led to the passage of the Sarbanes-Oxley Act.

Clare had recently gone to work for Saint Sebastian Catholic Hospital in Austin. She was uncertain whether the Sarbanes-Oxley Act applied to a not-for-profit Catholic hospital, so she asked her CEO a few questions. First, she asked if the hospital had a code of ethics that was reflective of the Sarbanes-Oxley Act. The CEO replied that they were required to have a code of ethics under JCAHO. He added that the code of ethics had been good enough for JCAHO at the last accreditation visit.

Next, Clare asked him some questions about the composition of the board of directors. In particular, she wanted to know how many of the board members had financial expertise. The CEO said that a majority of the board did not have financial backgrounds because other factors were deemed more important. He stated that there were three primary groups of board

members. One group of the board members was composed of representatives of Catholic orders who had deep understanding of ethical issues. This was essential to keep the hospital from getting on the wrong side of the Vatican with regard to obstetrical and gynecological issues. Another large group of board members was composed of wealthy philanthropists who contributed to the hospital. However, they had inherited their wealth and did not necessarily know anything about managing wealth. Last, a large group of board members was physicians who practiced at the hospital. It was essential to have them on the board to ensure their cooperation.

Last, Clare asked the CEO if the hospital kept financial data organized in such a way that it could identify major sources of revenues and expenses by customer. The CEO replied that he could not imagine why they would want to do that because all that was necessary was that the hospital provide good health care and conduct itself in a way that was consistent with Roman Catholic beliefs and values.

KEY ISSUES

Clare mulled over the CEO's answers. After work, she stopped by the Perry-Castaneda Library to research the Sarbanes-Oxley Act.

1. What would Clare find about the code of ethics required for a hospital?
2. What would Clare find about requirements for the composition of a board?
3. What would Clare find about the relationship between managerial accounting and internal controls?

CHECKLIST 1: The Sarbanes-Oxley Act	YES	NO
Governance		
Is a Section 302 governance report in place for your regulated health care entity?	o	o
Do you regularly review current governing board structure?	o	o
Do the board members sign the financial reports?	o	o
Do the board members certify that there are no false statements in the financial reports?	o	o
Do the board members certify that the financial statements are materially correct?	o	o
Has your board established the following committees:		
– An audit committee?	o	o
– A compensation committee?	o	o
– A nominating committee?	o	o
Does the hospital compensate the members of the board of directors?	o	o
Does the hospital provide education for the board of directors?	o	o
Has the hospital increased the proportion of board members capable of financial analysis?	o	o
Has the board met with your directors' and officers' (D&O) insurance carrier?	o	o
Has your controller, CFO, CEO, and/or internal auditors read the Treadway Commission report?	o	o
Internal Controls		
Is a Section 404 internal control report in place and filed annually?	o	o
Do the board members certify that internal controls are adequate to detect material errors?	o	o
Do the board members certify that they have recently tested the adequacy of internal controls?	o	o

Do the board members report on their conclusions about the effectiveness of internal controls based on the tests?	o	o
Is the internal control software sufficiently robust and flexible that it will still work after significant changes in operations?	o	o
Has the hospital established channels for complaints or anonymous tips from whistleblowers?	o	o
Do you outsource whistleblower compliance and treatment?	o	o
Ethics		
Is a Section 406 ethics policy report in place?	o	o
Has the hospital updated its code of ethics to reflect the Sarbanes-Oxley Act?	o	o
Did you have someone independently review your corporate code of ethics?	o	o
Does the hospital take steps to develop and maintain a culture of compliance?	o	o
Do you maintain ethics and compliance coordination with your HR department?	o	o
Disclosure		
Does the hospital have a Section 409 policy on disclosure?	o	o
Does the policy require disclosure of material changes of financial position or operations?	o	o
Does the hospital scrutinize prospective board members for conflicts of interest?	o	o
Does the hospital treat physicians the same as other board members?	o	o
Do you have regular follow-up with outside and internal legal counsel?	o	o
Finance		
Are all revenue streams consistently documented and accounted for?	o	o
Is revenue being properly allocated?	o	o
Do you understand the civil and criminal penalties of noncompliance and fraud?	o	o

Are these cited in text, or should they be in alphabetical order as a bibliography? Some entries are anecdotal (e.g., "Information on the Emergency Preparedness..."); should these be footnotes tied to specific points in text?

BIBLIOGRAPHY

Please confirm the changes from "Additional References" to "Bibliography" section.

U.S. Congress. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001. 107th Congress of the United States of America. H.R. 3162. 2002; http://Thomas.LOC.gov. Pub. L. No. 107-56.

U.S. Congress. The Sarbanes-Oxley Act of 2002. 107th Congress of the United States of America. H.R. 3763. 2002; http://Thomas.LOC.gov. Pub. L. No. 107-204.

See http://frwebgate.access.gpo.gov/cgi-in/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf.

www.whitehouse.gov/infocus/patriotact.

Preimestberger, C. "Why Disaster Recovery Isn't Optional Anymore." *eWeek* 28:12 (July 2011).

Melnick, S. V. "Accountants' Anti-Money-Laundering Responsibilities." *The CPA Journal* 73:12 (2003): 50–51.

Larson, R. K. and Herz, P. J. "Accountants, Corruption, and Money Laundering." *The CPA Journal* 73:6 (2003): 34–36.

Wetter, D. C., Daniell, W. D. and Treser, C. D. "Hospital Preparedness for Victims of Chemical or Biological Terrorism." *American Journal of Public Health* 91 (2001): 710–716.

Is this a footnote? None in text.

DHS published its Chemicals of Concern List on November 7, 2007. 6 C.F.R. Part 27, Appendix A.

Frist, B. "A Time for Preparedness." *Modern Healthcare* 32:51 (2005): 19.

Is this a footnote? None in text.

Information on the Emergency Preparedness Resource Inventory (EPRI) can be accessed at www.ahrq.gov/research/epri/index.html.

Cutlip, K. "Strengthening the System: Joint Commission Standards and Building on What We Know." *Hospital Topics* 80:1 (2002): 24–28.

Allen, K., Price, P. and Stevens, J. "Minimizing the Consequences of Disaster." *Healthcare Purchasing News* 27:4 (2003): 81–82.

Murphy, J. K. "After 9/11: Priority Focus Areas for Bioterrorism Preparedness in Hospitals." *Journal of Healthcare Management* 49:4 (2004): 227–235.

Andrews, J. "It's Always Orange Alert for Health Facility Security." *Healthcare Purchasing News* 27:5 (2003): 14–15.

Moss, B. "Getting Personal: Biometric Security Devices Gain Access to Health Care Facilities." *Health Facilities Management* 15:9 (2002): 21–24.

Glabman, M. "Bioterrorism: The Silent Killer." *Trustee* 54:10 (2001): 30.

USA PATRIOT Act §1016(d)(1). An ISAC acts as a centralized and confidential avenue for the critical infrastructures of North America, concentrating on sharing security issues and solutions within a particular industry sector. The Presidential Decision Directive 63 (PDD63), Homeland Security Presidential Directive (HSPD-7) and Executive Order 13231 (EO-13231) served as catalysts to the promotion of a concentrated effort regarding the sharing of various sector issues leading to unified and strengthened industry sectors. The IT-ISAC provides users with real-time information about urgent alerts, security news, vulnerabilities, viruses and other Internet threats, thus providing a coherent picture of the current state of the Internet threat to IT-ISAC members. The purpose of the IT-ISAC is also to provide a forum for sharing threat-related information, and ways to protect against those threats. Members can submit vulnerability, virus and general notifications for distribution. ISACs are non-profit organizations. The IT-ISAC is a Limited Liability Corporation (LLC) serving the Information Technology Sector owned by those within the IT sector who wish to participate as active members.

Is this a footnote? None in text.

www.it-isac.org/.

Karnow, C. "Launch on Warning: Aggressive Defense of Computer Systems." *Journal of Internet Law* 7:1 (2003): 9–14.

Adapted from: www.Mott.org.

US Congress. The Sarbanes-Oxley Act of 2002. 107th Congress of the United States of America. H.R. 3763. 2002; http://Thomas.LOC.gov. Public Law 107-204.

Steinberg, S. H. "What Does a Hospital Trustee Do?" *Physician's News Digest* (2005). (See http://physiciansnews.com/business/1005steinberg.html.)

Gerrish, J. C. "Ten New Commandments for Corporate Governance." *ABA Banking Journal* 94:11 (2002): 16–20.

Beasley, M. S. and Hermanson, D. R. "Going Beyond Sarbanes-Oxley Compliance: Five Keys to Creating Value." *The CPA Journal* 74:6 (2004): 11–13.

Ok to have two references together?

Daulerio, A. J. "Panelists: Nonprofits Should Brace for Sarbanes-Oxley Spillover." *The Bond Buyer* 36:31758 (2003): 4. (See also, Greene, J. "What Every Board Needs to Know." *Trustee* 57:6 (2004): 9–12.)

Grobmyer, J. E. and Reilly, G. "Good Governance: Ensuring the Financial Health of Your Hospital." *Trustee* 568 (2003): 32–33.

Unkovic, D. "A New Model for Health Care Boards." *Trustee* 57:1 (2004): 27–28.

Sarbanes-Oxley Act § 404(a)(1)–(2).

Harrington, C. "The New Accounting Environment." *Journal of Accountancy* 196:2 (2003): 28–33.

Bloch, G. D. "Sarbanes-Oxley's Effect on Internal Controls for Revenue." *The CPA Journal* 73:4 (2003): 68–70.

Winters, B. I. "Choose the Right Tools for Internal Control Reporting." *Journal of Accountancy* 197:2 (2004): 34–40.

OK to have two references together? Also, publication information for the second reference is needed.

O'Hare, P. K. "Sarbanes-Oxley Raises Red Flag for Not-for-Profits." *Healthcare Financial Management* 56:10 (2002): 42–44. (See also Green, J. "Not-for-Profit Hospitals Use Sarbanes-Oxley to Strengthen Their Boards' Financial Accountability." (2005)).

www.hhnmag.com/hhnmag_app/hospitalconnect/search/article.jsp?dcrpath=HHNMAG/PubsNewsArticle/data/0506HHN_FEA_NotForProfit&domain=HHNMAG.

Jaklevic, M. C. "Letting the Sunshine in." *Modern Healthcare* 33:12 (2003): 26–28.

Thallner, K. A. "High-Profile Cases Generate Interest in Corporate Responsibility: Exploring the Impact That Recent Events Will Have on Health Care." *Journal of Health Care Compliance* 4:5 (2002): 14–18.

Nelson, L. "Stepping into Continuous Audit." *Internal Auditor* 61:2 (2004): 27–29.

Grace, H. S. and Haupert, J. E. "Financial Officers' Code of Ethics: Help or Hindrance?" *The CPA Journal* 73:3 (2003): 65–66.

Myers, R. "Ensuring Ethical Effectiveness." *Journal of Accountancy* 195:2 (2003): 28–33.

Messmer, M. "Sarbanes-Oxley Act: What Does It Mean To Me?" *Strategic Finance* 84:9 (2003): 13–14.

Is this a footnote? Citation in text not found.

The Joint Commission was formerly known as the Joint Commission on Accreditation of Healthcare Organizations or JCAHO.

Malz, A. "Code of Ethics in the Wake of Sarbanes-Oxley." *Trustee* 56:10 (2003): 31.

OK to have two references together?

Gantner, J. J. "Executive Insights." *Healthcare Financial Management* 57:4 (2003): 32–36. (See also Jaklevic, M. C. "Conflict Resolution." *Modern Healthcare* 34:12 (2004): 22.)

Sarbanes-Oxley Act § 409.

Barrett, R. "Disclosure: The Real Challenge of Sarbanes-Oxley." *The CPA Journal* 74:1 (2004): 11.

Haugh, R. "The Benefits of Transparency." *Hospitals and Health Networks* 77:10 (2003): 16.

Gantner, J. J. "Executive Insights." *Healthcare Financial Management* 57:4 (2003): 32–36.

Tyler, L. L. and Biggs, L. L. "Conflict of Interest: Strategies for Remaining Purer than Caesar's Wife." *Trustee.* 57:3 (2004): 24–26.

DiMaggio, P. J. and Powell, W. W. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48:2 (1983): 147–160.

Is this a footnote or a reference?

See "Non Profit Hospitals Take Action to Comply with Sarbanes-Oxley" at www.insidesarbanesoxley.com/2006/02/non-profit-hospitals-take-action-to.asp.

O'Hare, P. K. "Sarbanes-Oxley Raises Red Flag for Not-for-Profits." *Healthcare Financial Management* 56:10 (2002): 42–44.

www.philanthropyjournal.org.

Please verify this reference.

Balle, D. "Ernst & Young: Healthcare Provider Sector Outlook." *Sarbanes-Oxley Compliance Journal* February 1, 2007. See www.s-ox.com/dsp_getNewsDetails.cfm?CID=1980.

www.fticonsulting.com.

Rosen, B. F. and Bresnick, M. L. Special to the *Daily Record.* January 18, 2008. See www.mddailyrecord.com/article.cfm?id=140707&type=Daily.

Marcinko, D. E. and Hetico, H. R. The US Patriot Act. In Marcinko, D. E. (editor). *The Business of Medical Practice.* Springer Publishing, New York, 2011.

Royo, M. B. and Nash, D. B. "Sarbanes-Oxley and Not-for-Profit Hospitals: Current Issues and Future Prospects." *American Journal of Medical Quality* 23:1 (February 2008): 70–72. See http://ajm.sagepub.com/cgi/content/citation/23/1/70.